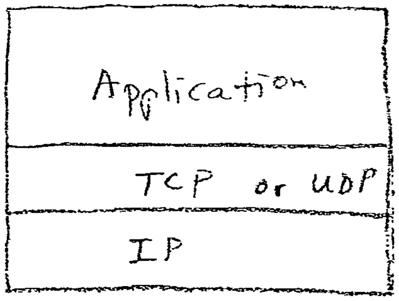


FIG. 1A
(prior art)

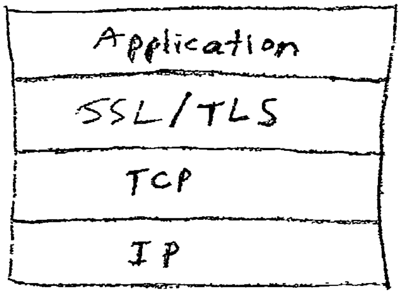


FIG. 1B
(prior art)

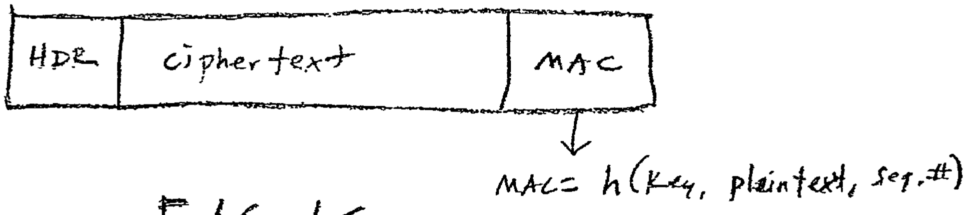


FIG. 1C
(prior art)

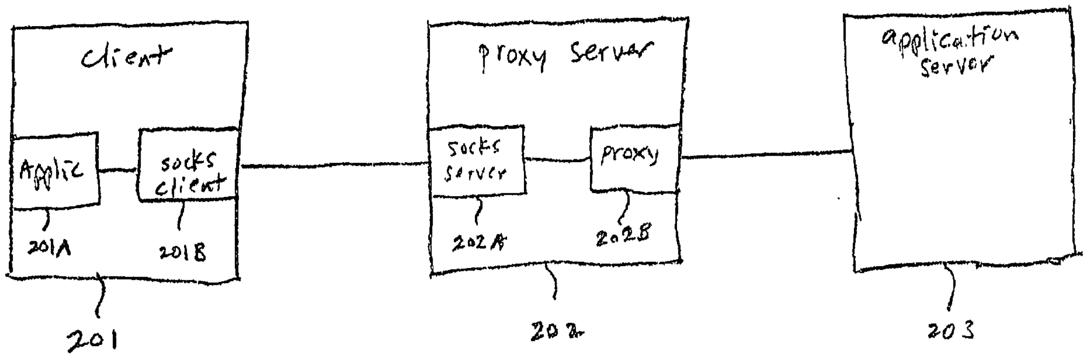


FIG. 2
(prior art)

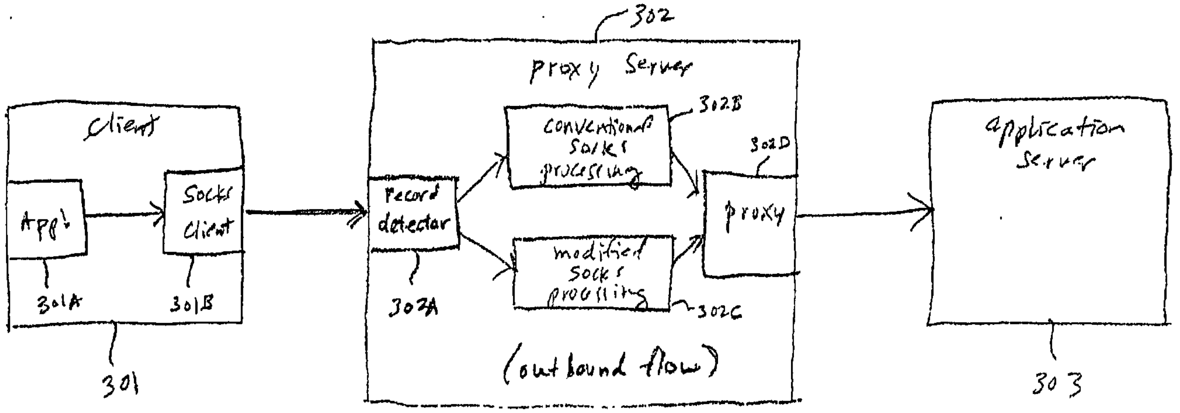

302
client
App'l
301A
Socks client
301B
301
proxy Server
record detector
302A
conventional Socks processing
302B
modified Socks processing
302C
proxy
302D
(outbound flow)
application Server
303

FIG. 3A

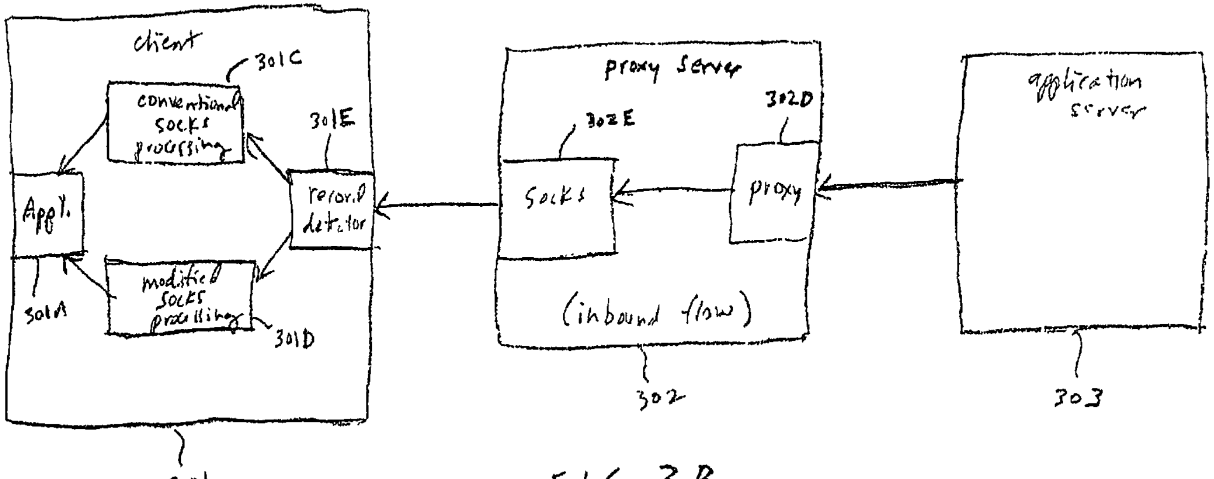

client
301C
conventional socks processing
301E
record detector
Appl.
301A
modified socks processing
301D
301
proxy Server
302E
Socks
302D
proxy
(inbound flow)
302
application server
303

FIG. 3B

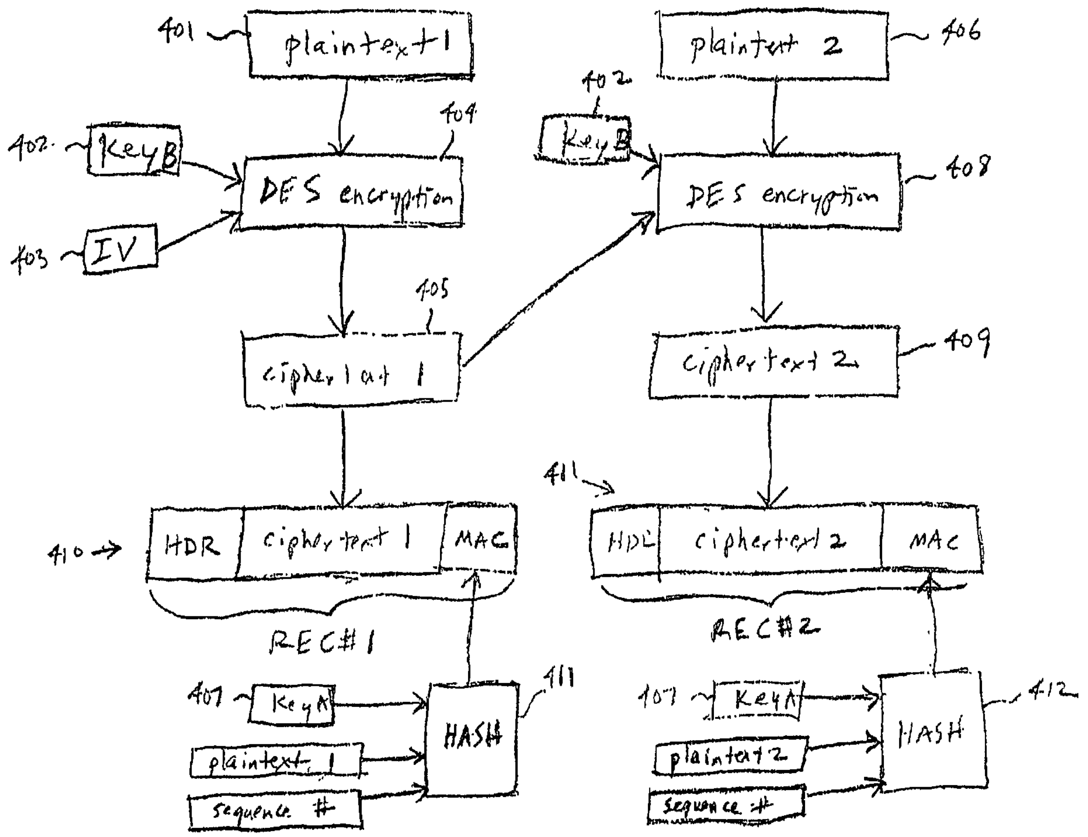


FIG. 4A
(prior art)

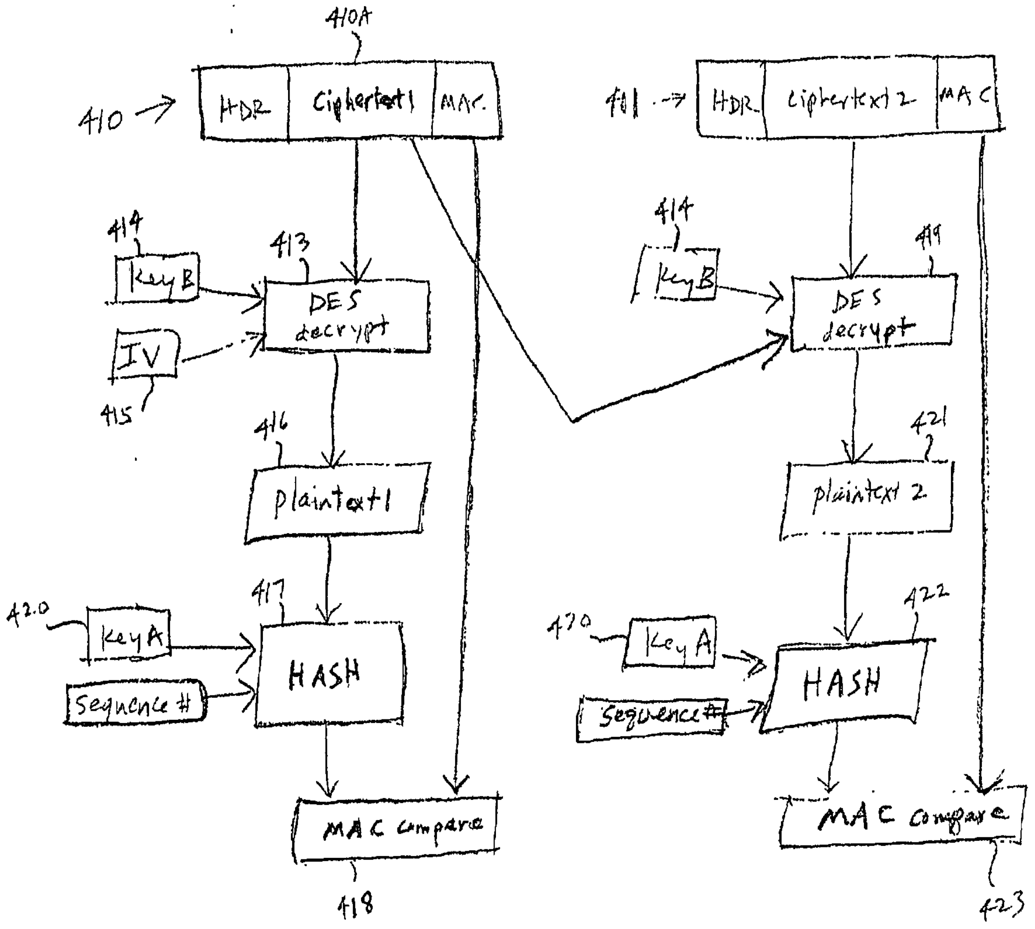
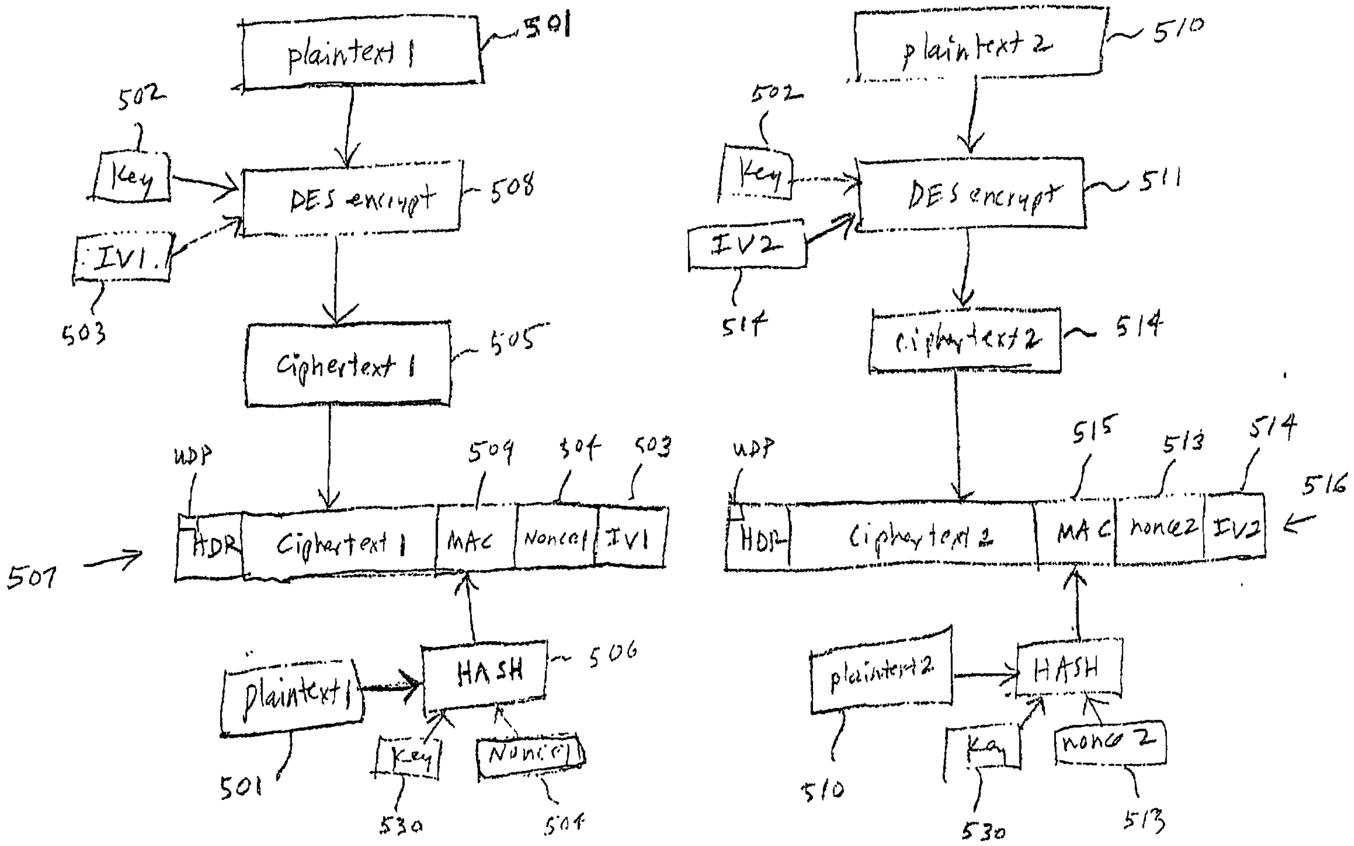


FIG. 4B
(prior art)



plaintext 1
501
502
Key
DES encrypt
508
IV1
503
Ciphertext 1
505
UDP
509
504
503
507
HDR
Ciphertext 1
MAC
Nonce1
IV1
plaintext1
HASH
506
Key
Nonce1
501
530
504
plaintext 2
510
502
Key
DES encrypt
511
IV2
517
ciphertext 2
514
UDP
515
513
514
516
HDR
Ciphertext 2
MAC
nonce2
IV2
plaintext2
HASH
Ka
nonce 2
510
530
513

FIG. 5A

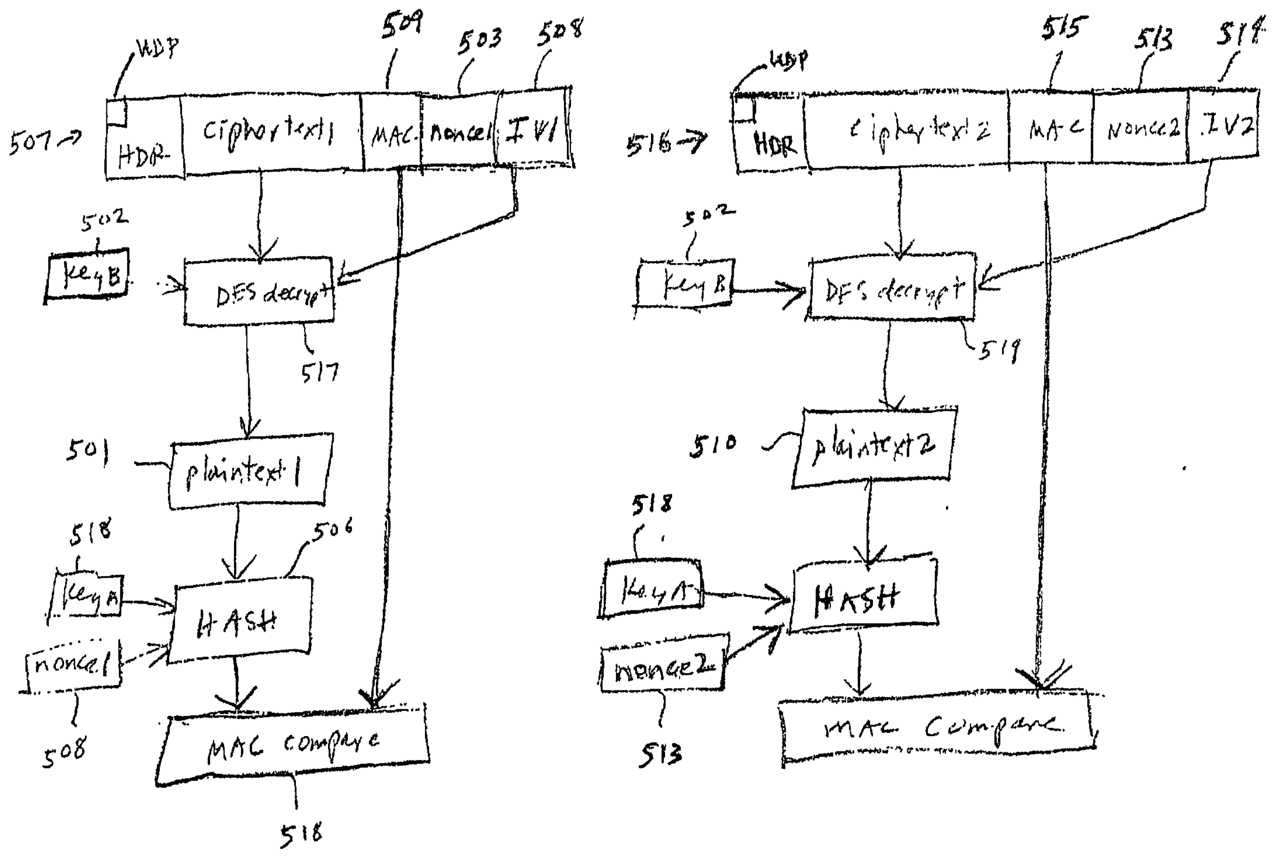

UDP
509
503
508
507
HDR
ciphertext1
MAC
nonce1
IV1
502
keyB
DES decrypt
517
501
plaintext1
518
keyA
506
HASH
nonce1
508
MAC compare
518
UDP
515
513
514
516
HDR
ciphertext2
MAC
nonce2
IV2
502
KeyB
DES decrypt
519
510
plaintext2
518
KeyA
HASH
nonce2
513
MAC Compare

FIG. 5B

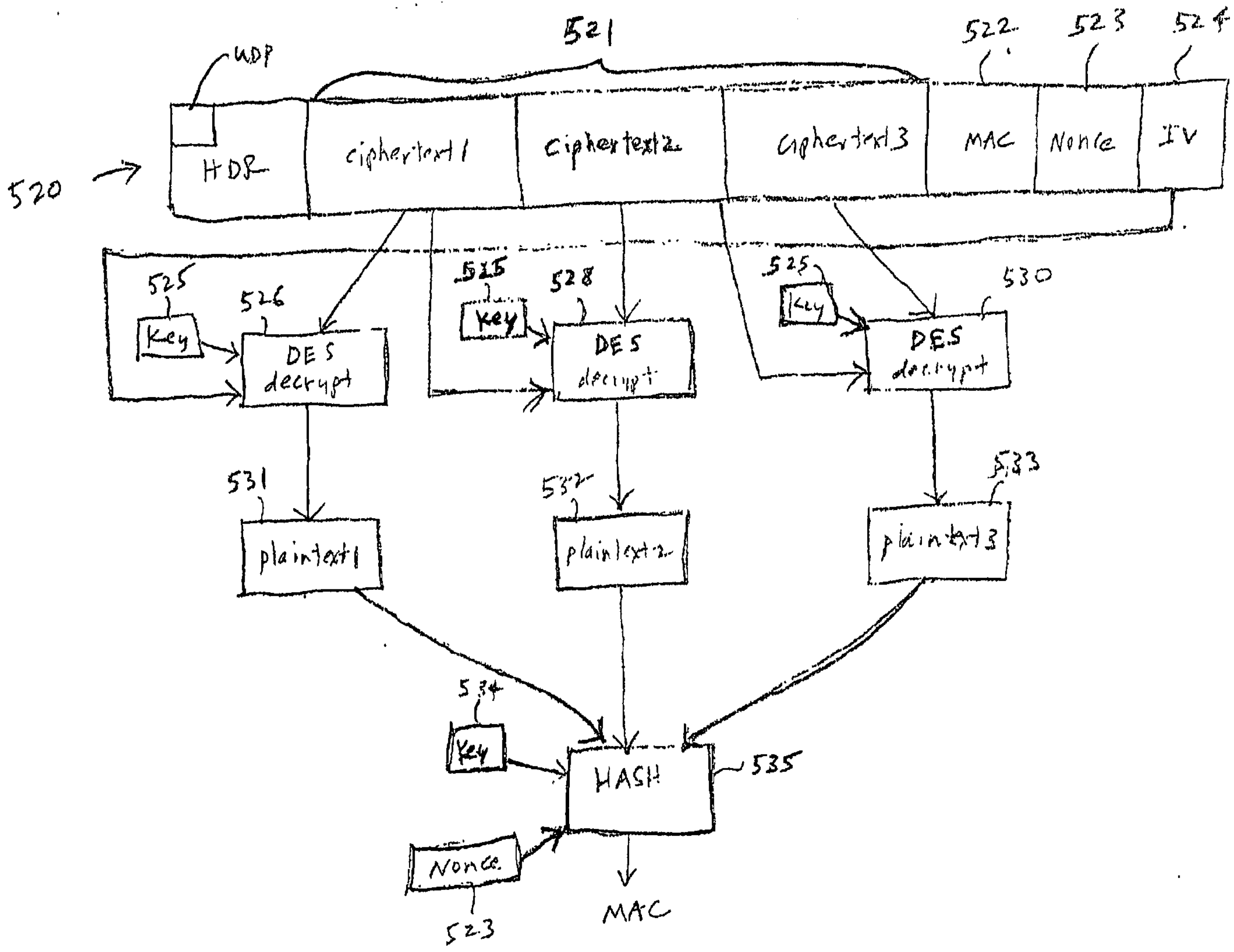
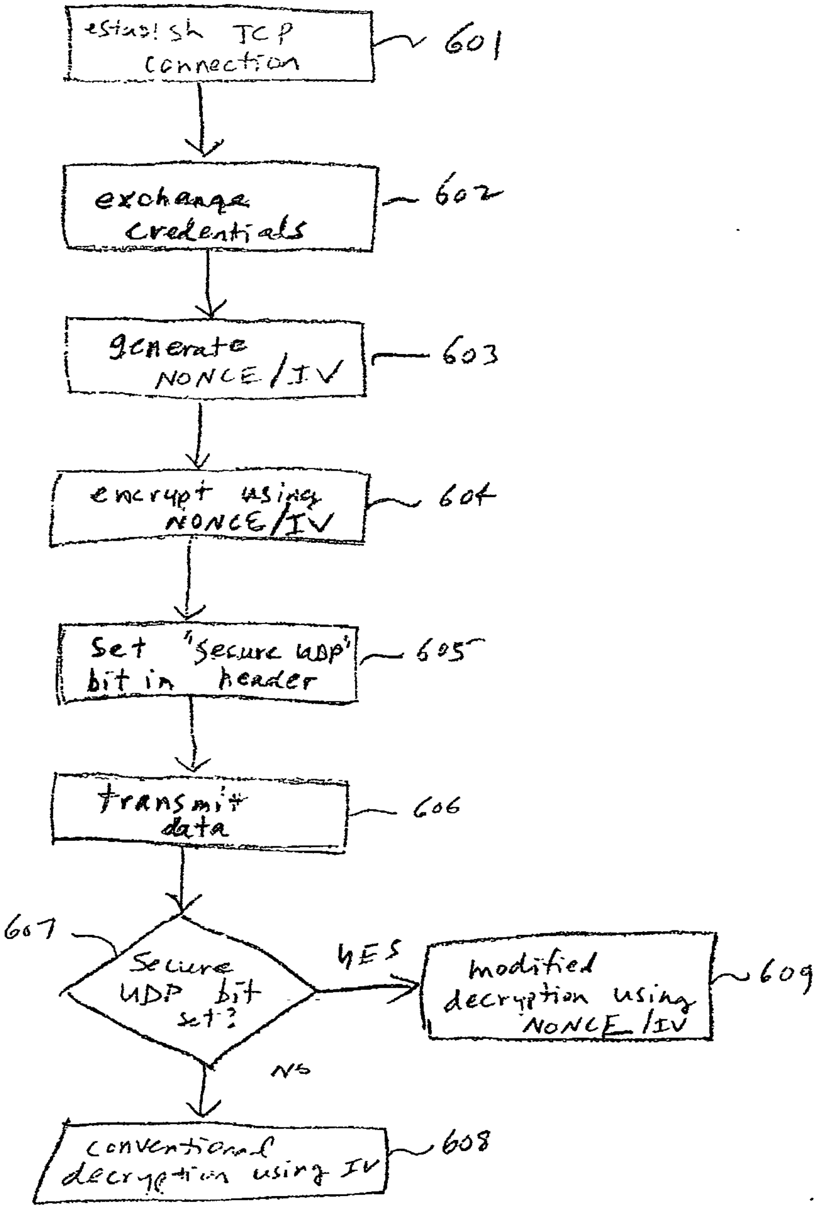

521
522
523
524
UDP
520
HDR
ciphertext1
ciphertext2
ciphertext3
MAC
Nonce
IV
525
Key
526
DES decrypt
515
Key
528
DES decrypt
525
Key
530
DES decrypt
531
plaintext1
532
plaintext2
533
plaintext3
534
Key
HASH
535
Nonce
523
MAC

FIG. 5C

FIG. 6


establish TCP connection
601
exchange credentials
602
generate NONCE/IV
603
encrypt using NONCE/IV
604
Set "secure UDP" bit in header
605
transmit data
606
607
Secure UDP bit set?
YES
modified decryption using NONCE/IV
609
NO
conventional decryption using IV
608